Christopher McLane, senior CBRN analyst, at the Joint Requirements Office for CBRN Defense, on enabling command and control in CBRN environments

The speed of need

"To succeed in the emerging security environment, our Department and Joint Force will have to out-think, out-manoeuvre, out-partner and out-innovate revisionist powers, rogue regimes, terrorists and other threat actors."
US 2018 National Defense Strategy

The key to success in any potential or actual CBRN environment is for the leader to rapidly understand that environment so they may make decisions and direct actions to respond. In view of this, the CBRN defence community has long recognised the need to automate CBRN warning and reporting, attack analysis, and decision making. Turning this goal of CBRN integrated early warning" (IEW) into reality, however, has proven elusive. The challenges of networking multiple CBR sensors into disparate network configurations and command and control (C2) systems are daunting. And this is merely the beginning. Once resident on the network, the raw data is of little use without user friendly analytical tools to process the data, provide information and ultimately facilitate understanding. All this must be accomplished while maintaining data integrity and security in the face of growing cyber threats.

In December 2019, the US Joint Staff Joint Requirements Office for CBRN Defense (JRO) started to work up a requirements development framework to meet the challenges posed by IEW capability development. The selected approach is termed CBRN support to command and control (CSC2).

As the name implies, CSC2 approaches the IEW as a C2 challenge. CSC2 is the enablement of situation awareness (SA) and C2 to continue military operations in an actual or threatened CBRN environment. At its end state, CSC2 will allow CBRN data and information transfer across networks and to the common operation picture (COP), enabling commanders to visualise the CBRN threat and provide direction in the context of the larger mission space.

CSC2 capability development is occurring in support of the US Chemical Biological Defence Programme (CBDP) CBRN IEW campaign. The objective of this campaign is to deliver capabilities to the Joint Force that enhance technical and tactical advantages by providing reliable, relevant warning of CBRN use and resulting hazards, enabling the force to maintain freedom of action in a CBRN environment. As mentioned, previous attempts to realise IEW have yielded limited success. So why now? Why is CSC2 different?

Within the US Department of Defense (DoD), recent changes and advances in policy, technology and practice have converged creating an opportunity to deliver CBRN information to leaders at the speed of need. It is recognised that the capability development cycle time, from inception to delivery, must decrease to keep pace

The Perceptive Dragon ATD series proved the utility and feasibility of integrating current and future CBR sensors with tactical communication networks ©DoD

DECON HAS NEVER BEEN SO EASY.

RAISE THE BAR

It's time to Raise the BAR for your decon SOPs.

Blot. Apply. Remove. **Any threat, any surface.** Changing the way you do decon is that simple. Hybrid Decon follows the BAR Method to quickly, efficiently, and effectively eliminate virtually any CBRNe threat.

The **Enhanced Decon System (EDS)™** is the only Hybrid Decon go-bag with the power of **Dahlgren Decon™** and **FiberTect®** to combat hundreds of known and emerging threats.

Raise the BAR for your decon SOPs. Learn more about the EDS by visiting **www.firstlinetech.com/EDS**

FLUA

Immersive online decontamination training now available on flightLMS!
First Line Utilization Academy (FLUA) is now accepting enrollment into all available courses. Scan to access the full course catalog and register for your first course today!

GET IN TOUCH
www.firstlinetech.com | sales@firstlinetech.com | +1.703.955.7510

FIRST LINE TECHNOLOGY

The speed of need

Joint Task Force Civil Support have been an early user of Joint All Domain C2 ©DoD

with a growing list of threats across the spectrum of conflict. This can only come from shortening the time required to identify promising technologies and approaches through S&T, and by developing requirements, and mature, developed and field-usable capabilities for end users.

This recognition has led to significant changes in acquisition policy that provide for more highly tailored purchasing based on the speed and type of capability required while recognising, embracing and mitigating attendant risks. At its core, CSC2 is information technology, and specifically, it is software focused.

The DoD's new adaptive acquisition framework provides a software acquisition pathway that facilitates rapid and iterative capability delivery in line with approaches used by the commercial information technology leaders. The pathway integrates modern software development practices such as agile software development, DevSecOps, and lean practices, then leverages active user engagement to rapidly and iteratively deliver working software to meet the highest priority user needs. The result is that users get the required capability in months, rather than years as with traditional approaches. These acquisition policy changes are accompanied by similar changes in requirements development with a focus on leaner, less prescriptive requirements using meaningful performance metrics. At the same time they're flexible enough for making cost, schedule and performance trade space decisions that would have taken months or years to earn approvals using the traditional approach.

Concurrent with these policy changes, materiel developers within the US chemical biological defense programme have proven the technological feasibility of CSC2. These efforts include successful technology demonstrations and deployments by the Defense Threat Reduction Agency (DTRA) and the Joint Program Executive Office for CBRN Defense (JPEO-CBRND). DTRA's chemical and biological technologies department has also conducted a series of demonstrations as part of its IEW advanced technology demonstration (ATD) programme. This Perceptive Dragon ATD series proved the utility and feasibility of integrating current and future CBR sensors with tactical communication networks and decision support tools to enable common battlefield awareness and understanding, and speed up leader decision making in static and mobile environments.

In collaboration with DTRA, the JPEO-CBRND has successfully transitioned multiple IEW-enabling technologies for advanced development. Among the most promising IEW capabilities to have been deployed to a forward operational area recently, were networked biological, chemical, force protection, and meteorological sensors across multiple installations. The sensor suite transfers data through a sensor management system and multiple communication modalities into a central node. This networked capability provides warfighters with near real time situational awareness and environmental understanding. Analytics monitor sub-threshold CB sensor data, real time meteorological data, and force protection information. This data and information is fused within an analytics application, which will track, map and project the hazard across the area of interest.

Finally, CSC2 development is not happening in a vacuum. In January 2020, the DoD established the Joint All Domain C2 (JADC2) cross-functional team as a three star joint governing body to lead DoD efforts to "rapidly realise agile and resilient C2 across all domains through integrated and synchronised capability development - execute inside the enemy's decision cycle."

JADC2 is the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance. It is not a programme of record; rather JADC2 provides structure, process and direction to meet DoD C2 imperatives. CSC2 development is occurring in parallel with the JADC2 initiative, and leverages and aligns with JADC2 lessons learned, best practices, and policy

updates in all requirements and materiel development. Taken as a whole, the changes and accomplishments described above combine to provide an unprecedented opportunity to deliver on the long desired outcome of CBRN IEW.

CSC2 capability development begins with a service and combatant command submission of capability needs through an online repository. The joint staff chartered the CSC2 sub-working group, which is composed of stakeholders from across the DoD, to review and prioritise these needs for potential development based on various factors including overall joint force value and technological feasibility. It is impossible to develop and field all needed capabilities simultaneously, and attempts to do so will fail. As such, CSC2 follows a time phased approach to requirements and capability development. Incremental progress is accepted and embraced. Initial requirements define limited objectives to achieve success, exercise new processes, and apply lessons learned iteratively. Emphasis is on lean, minimally prescriptive requirements that enable agile acquisition strategies. To facilitate and organise CSC2 capability development, plans call for four primary phases of capability development and deployment. Requirements are captured in documents called capability definition packages (CDP), each covering an increment of capability.

The joint staff J6 deputy director for cyber, and command, control, communication and computers integration approved CSC2 CDP 1 in February 2021. This CDP defines requirements for integrating CBR sensors into tactical C2 networks. A key tenet of the CSC2 approach to enabling CBRN IEW is reduction (or elimination) of time consuming, manual processes that hinder effective warning of existing or potential CBRN hazards, and slow leader decision making and direction. The first step in achieving this reduction is automated transfer of data from CBRN sensors through tactical communication networks for follow-on processing and analysis. CDP 1 focuses on realising this automated transfer. The architectural framework in which this transfer occurs will likely vary by service and the environment; however the initial data transfer will generally be from sensors to a sensor controller/manager (SCM). The SCM will typically be software resident on an existing or dedicated manned, networked platform.

Looking to the future, plans call for CSC2 capability to build out over time, with three additional phases of follow-on capability development planned. Phase two will focus on integration, visualisation, and analysis of data accrued at tactical and operational levels; initial integration of operational, open source, and environmental health information; development of decision support tools for operational planning in a CBRN environment; initial integration of capabilities into service computing environments and COPs. Information sharing with domestic partners is also included. The third development phase will continue expansion of CSC2 capability. Planned capabilities include CBRN operational decision support tools; expanded integration of RN sensing and analysis; continued integration into service and joint networked computing environments and COEs/COPs. Partner and coalition data and information sharing will occur via existing network mechanisms and protocols. The final planned phase fully integrates CSC2 capabilities into joint/service COEs/COPs, and continues integration of environmental/health monitoring information to enable IEW decision support tools using artificial intelligence and machine learning.

The key to success in any potential CBRN environment is to rapidly understand that environment so leaders may make informed decisions ©DoD